

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Atsushi Fujioka et al.

Serial No. To be assigned

Art Unit: To be assigned

Filed: Herewith

Examiner: To be assigned

For: ELECTRONIC VOTING
METHOD AND SYSTEM AND
RECORDING MEDIUM HAVING
RECORDED THEREON A
P R O G R A M F O R
IMPLEMENTING THE METHOD

Atty Docket: 162/534

jc511 U.S. PTO

09/434440



**SUBMISSION OF CERTIFIED PRIORITY DOCUMENT(S) and
CLAIM TO PRIORITY UNDER 35 U.S.C. § 119**

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Priority under 35 U.S.C. § 119 is hereby claimed to the following priority document(s), certified copies of which are enclosed. The documents were filed in a foreign country within the proper statutory period prior to the filing of the above-referenced United States patent application.

<u>Country</u>	<u>Priority Document Serial No.</u>	<u>Filing Date</u>
Japan	10-320173	November 11, 1998

Acknowledgement of this claim and submission in the next official communication is respectfully requested.

Respectfully submitted,

Morris Liss, Reg. No. 24,510
Pollock, Vande Sande & Amernick, R.L.L.P.
1990 M Street, N.W.
Washington, D. C. 20036-3425
Telephone: 202-331-7111

Date: 11/5/99

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

JCS11 U.S. PTO
09/434440
11/05/99

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

1 9 9 8 年 1 1 月 1 1 日

出 願 番 号
Application Number:

平成 1 0 年 特 許 願 第 3 2 0 1 7 3 号

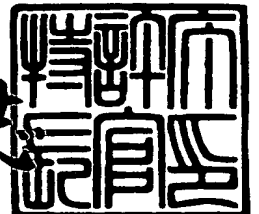
出 願 人
Applicant (s):

日本電信電話株式会社

1 9 9 9 年 8 月 1 6 日

特 許 庁 長 官
Commissioner,
Patent Office

伴 佐 山 建 志



出 証 番 号 出 証 特 平 1 1 - 3 0 5 7 2 5 2

【書類名】 特許願

【整理番号】 NTTH106401

【提出日】 平成10年11月11日

【あて先】 特許庁長官殿

【国際特許分類】 G07C

【発明の名称】 電子投票方法、装置及びプログラム記録媒体

【請求項の数】 6

【発明者】

 【住所又は居所】 東京都新宿区西新宿三丁目19番2号 日本電信電話株式会社内

 【氏名】 藤岡 淳

【発明者】

 【住所又は居所】 東京都新宿区西新宿三丁目19番2号 日本電信電話株式会社内

 【氏名】 阿部 正幸

【発明者】

 【住所又は居所】 東京都新宿区西新宿三丁目19番2号 日本電信電話株式会社内

 【氏名】 三浦 史光

【特許出願人】

 【識別番号】 000004226

 【氏名又は名称】 日本電信電話株式会社

【代理人】

 【識別番号】 100066153

 【弁理士】

 【氏名又は名称】 草野 卓

【選任した代理人】

 【識別番号】 100100642

 【弁理士】

【氏名又は名称】 稲垣 稔

【手数料の表示】

【予納台帳番号】 002897

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9806848

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 電子投票方法、装置及びプログラム記録媒体

【特許請求の範囲】

【請求項 1】 投票者は、投票内容を暗号化器を用いて暗号化し、その暗号化投票内容を、乱数発生器を用いて生成した乱数成分とともに攪乱器に入力して攪乱された投票文を作成し、この投票文を選挙管理者装置に送信し、

選挙管理者は、投票者の確認を行った後に、受信した投票文を署名作成器に入力して投票文の署名を生成し、これを投票者装置に送り返し、

投票者は、受信した投票文の署名を乱数成分除去器に入力し、乱数成分の影響を取り除いて暗号化投票内容の署名情報を求め、その署名情報と上記暗号化投票内容装置へ送信し、

集計者は、暗号化投票内容と受信した署名情報を署名検査器に入力して投票文が選挙管理者によって署名されていることを確認し、暗号化投票内容を表にしてこれを周知し、

投票者は、自分の暗号化投票内容が表に存在することを確認し、

集計者は、復号器を用いて暗号化投票内容を復号して開票を行う電子投票方法

【請求項 2】 集計者とその装置を複数置き、それぞれが備える復号器を用いて開票を行うことを特徴とする請求項 1 記載の電子投票方法。

【請求項 3】 複数ある復号器の中の一定数のものだけを用いて開票を行えることを特徴とする請求項 2 記載の電子投票方法。

【請求項 4】 投票者装置と、選挙管理者装置及び集計者装置とがそれぞれ通信路で接続され、

投票者装置は、

投票内容を集計者装置の暗号化鍵で暗号化する暗号化器と、

乱数を発生する乱数発生器と、

上記暗号化投票内容と上記乱数を攪乱して投票文を作成する攪乱器と、

上記投票文の署名を生成する署名作成器と、

上記投票文及びその署名を選挙管理者装置へ送信する手段と、

選挙管理者装置から受信した投票文署名から乱数成分の影響を取り除いて暗号化投票内容の署名情報を求める乱数成分除去器と、

上記暗号化投票内容の署名情報を検証する署名検査器と、

その署名検査器の検証に合格すると上記暗号化投票内容署名情報及び上記暗号化投票内容を集計者装置へ送信する手段と、

集計者装置から受信した投票内容一覧表に自己の暗号化投票内容が存在するか否かを検査する検査器とを備え、

選挙管理者装置は、

投票者装置から受信した投票文及びその署名を検証する署名検査器と、

その検証に合格すると、上記受信した投票文を入力して投票文の署名を生成する署名作成器と、

上記投票文の署名を投票者装置へ送信する手段とを備え、

集計者装置は、

投票者装置から受信した暗号化投票内容と暗号化投票内容の署名情報を入力して署名を検証する署名検査器と、

その検証に合格すると各投票者装置から受信した暗号化投票内容の表を作成する表作成器と、

暗号化投票内容を復号して開票する復号器とを備える
ことを特徴とする電子投票システム。

【請求項5】 電子投票システムに用いられる投票者装置であって、

投票内容を集計者装置の暗号化鍵で暗号化する暗号化器と、

乱数を発生する乱数発生器と、

上記暗号化投票内容と上記乱数を攪乱して投票文を作成する攪乱器と、

上記投票文の署名を生成する署名作成器と、

上記投票文及びその署名を選挙管理者装置へ送信する手段と、

選挙管理者装置から受信した投票文署名と上記乱数を入力して投票文署名から乱数成分の影響を取り除いて暗号化投票内容の署名情報を求める乱数成分除去器と、

上記暗号化投票内容の署名情報と上記暗号化投票内容を入力して、上記暗号化

投票内容の署名情報を検証する署名検査器と、

その署名検査器の検証に合格すると上記暗号化投票内容の署名情報及び上記暗号化投票内容を集計者装置へ送信する手段と、

集計者装置から受信した投票内容一覧表に自己の暗号化投票内容が存在するかどうかを検査する検査器とを備える投票者装置。

【請求項6】 電子投票システムの投票者装置のコンピュータが実行するプログラムを記録した記録媒体であって、

投票内容を集計者装置の暗号化鍵で暗号化する処理と、

乱数を発生する処理と、

上記暗号化投票内容と上記乱数を攪乱して投票文を作成する処理と、

上記投票文の署名を生成する処理と、

上記投票文及びその署名を選挙管理者装置へ送信する処理と、

上記乱数を用いて、選挙管理者装置から受信した投票文署名から乱数成分の影響を取り除いて暗号化投票内容の署名情報を求める処理と、

上記暗号化投票内容を用いて、上記暗号化投票内容の署名情報を検証する処理と、

その検証に合格すると上記暗号化投票内容署名情報及び上記暗号化投票内容を集計者装置へ送信する処理と、

集計者装置から受信した投票内容一覧表に自己の暗号化投票内容が存在するかどうかを検査する処理とを

上記コンピュータが実行するプログラムを記録した記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、電気通信システムでアンケート調査等を行う場合に、安全で、かつ、公平な無記名投票を実現しようとする電子投票システム、投票方法及びプログラム記録媒体に関する。

【0002】

【従来の技術】

無記名投票は、投票者と投票内容の対応を秘密にでき、個人の思想信条に関するプライバシーを守るのに適しているので、電子会議やCATV等の双方向通信でのアンケート調査等に利用できる。

電気通信において、安全で、かつ、公平な無記名投票を行うには、投票者の偽装や二重投票、投票文の盗聴に伴う投票内容の漏洩等の防止が必要である。これらの問題を解決する方法として、デジタル署名を用いた電子投票方式が提案されており、例えば、Atsushi Fujioka, Tatsuaki Okamoto, Kazuo Ohta: "A practical secret voting scheme for large scale elections", in Advances in Cryptology-AUSCRYPT'92, Lecture Notes in Computer Science 718, Springer-Verlag, Berlin, pp.244-251(1993)、特願平4-170899号「電子投票方法および装置」がある。

【0003】

しかしながら、この方法には、いくつかの欠点が存在する。

まず、投票者が投票締切後に自分の投票を確認し、再度復号化鍵を集計者に送信することが必要であり、すなわち、投票者の利便性の低いシステムである。

また、集計者は単独であり、耐故障性の低いシステムである。

【0004】

【発明が解決しようとする課題】

この発明の目的は、プライバシーを侵すことなく異議申し立てが行え、集計の途中経過が投票に影響を与えず、また、集計者の不正や機能不全に対処できる、安全、公平、かつ、簡便な電子投票システム及びその方法を構築することにある。

【0005】

【課題を解決するための手段】

この発明では、投票者が投票内容を集計者の暗号化鍵で暗号化し、さらにその暗号化投票内容を乱数で攪乱して投票文を作成して、その投票文に署名を付けて選挙管理者に送信する。選挙管理者は、付加された署名を用いて投票者の正当性を認証した後に、投票文に署名して投票文の署名を各投票者に送り返す。投票者は投票文の署名から乱数の影響を取り除いて投票文の署名情報を求め、集計者に

送信する。集計者は受信した投票文の署名情報が選挙管理者によって署名されていることを確認した後に、投票文を暗号化されたまま公開する。それぞれの投票者が、公開された投票文の一覧表に自分の投票文が登録されていることを確認した後に、集計者は、自らが保持する復号化鍵を用いて投票文からすべての投票内容を取り出し、これを集計する。もし、登録されていない場合には、集計者に対して異議を申し立てる。また、集計者を複数とし、それぞれが復号化鍵の一部を保持し、集計者全員もしくは一定数が協力することによって、投票文からすべての投票内容を取り出すこともできるとする。

【0006】

まず、投票文は投票内容を乱数で攪乱しているので、選挙管理者、および集計者は、攪乱された投票文から投票内容を求めることが出来ず、投票の無記名性が保障できる。

ここで、復号化鍵は集計者が保持しており、投票者は、開票のために再度集計者へ通信を行なう必要がない。

【0007】

以上より、この発明では、従来より指摘されていた投票者の利便性の問題を解決できる。

次に、集計者を複数とし、それらが協力することにより暗号化された投票文を開票する場合は、異議申し立て時に、自分が正当な投票者であることは、暗号化されている投票文と選挙管理者の署名を送るだけで示すことができる。すなわち、複数存在する集計者の一部に不正者が存在したとしても、全員もしくは一定数の集計者が協力しないかぎり投票内容が明らかになることはない。

【0008】

また、分散された集計者には、暗号化された投票内容が集まるので、この場合も全員もしくは一定数の集計者が協力しないかぎり、投票の間にその途中経過は明らかにならないので、公平な投票方式となっている。

さらに、集計者全員でなく一定数が協力するだけで開票が可能な場合は、集計者内の何人かが不正者、もしくは、開票への協力が不可能となっても、正しく開票作業を行なうことができるので、この方式は耐故障性の高いシステムであると

言える。

【0009】

【発明の実施の形態】

以下に、この発明の第一の実施例について説明する。

図1aはこの発明の全体構成を示す図である。T人の投票者の装置（投票者装置）100は、選挙管理者の装置（選挙管理者装置）200と、また集計者の装置（集計者装置）300と、それぞれ記名通信路400、および匿名通信路500を介して結合されている。また、集計者は投票内容の一覧表600を公開し、投票者は全員、これにアクセスが可能であるとする。図2にこの発明の投票システムにおける通信シーケンス例を示し、以下、それぞれ、図3に投票者装置100の構成例を、図4に選挙管理者装置300の構成例を、図5に集計者装置400の構成例を示す。また、図1bに投票後の投票内容の一覧表を、図1cに集計後の投票内容の一覧表を例示する。

【0010】

以下では、特に投票者 V_i が投票内容 v_i を選挙管理者Aの承認を得た後に、集計者Cに対して投票する場合について説明する。

ここで、簡単のため、以下のような記法を用いる。

$x = \xi_C(v)$: 集計者Cの暗号化関数 (v : メッセージ)

$v = \rho_C(x)$: 集計者Cの復号化関数 (x : 暗号文)

$s = \sigma_i(m)$: 投票者 V_i の署名作成関数 (m : メッセージ)

$m = \zeta_i(s)$: 投票者 V_i の署名検証関数 (s : 署名)

$s = \sigma_A(m)$: 選挙管理者Aの署名作成関数 (m : メッセージ)

$m = \zeta_A(s)$: 選挙管理者Aの署名検証関数 (s : 署名)

$e = \omega_A(m, r)$: 攪乱関数 (m : メッセージ、 r : 乱数)

$y = \delta_A(d, r)$: 乱数成分除去関数 (d : 署名、 r : 乱数)

ここで、選挙管理者の署名関数 (δ_A , ζ_A) は、乱数による攪乱 (ω_A)、および、乱数成分除去 (δ_A) ができるものとする。

【0011】

このような署名関数については、例えばRSA暗号の暗号化関数と復号化関数

があり (Ronald Rivest, Adi Shamir, Leonard Adleman: "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, Vol.21, No.2, pp.120-126(Feb., 1978)), 乱数による攪乱の手法についての詳細は、David Chaum: "Security without identification: Transaction systems to make big brother obsolete", Communications of the ACM, Vol.28, No.10, pp.1030-1044(Oct., 1985)に記述されている。

【0012】

以下、この発明の第一の実施例における投票の手順を示す。

Step 1 投票者 V_i は、投票者装置 100 により投票の準備を以下のように行う。

Step 1-1 投票者 V_i は、投票内容 v_i を暗号化器 110 で集計者 C の暗号化関数により暗号化し、投票用紙 x_i

$$x_i = \xi_C (v_i)$$

を作成する。

【0013】

Step 1-2 投票者 V_i は、乱数生成器 120 を用いて乱数 r_i を生成し、攪乱器 130 を用いて x_i 、 y_i を攪乱して e_i

$$e_i = \omega_A (x_i, r_i)$$

を作成する。

Step 1-3 投票者 V_i は、署名作成器 140 を用いて、 e_i の署名 s_i

$$s_i = \sigma_i (e_i)$$

を作成し、 $\langle e_i, s_i \rangle$ を選挙管理人 A の装置 200 に送信する。

Step 2 選挙管理者 A は、選挙管理者装置 200 により承認手続きを以下のように行う。

【0014】

Step 2-1 選挙管理者 A は、投票者が有権者であることを、予め用意された有権者リストにあるか否かを投票権確認手段 210 により調べて確認する。
もし、そうでなかったら、選挙管理者 A は承認を拒否する。

Step 2-2 選挙管理者 A は、これ以前に投票者 V_i が選挙管理者 A による承認

を受けているか否かを、投票者リストに V_i があるかを投票権確認手段210により調べて検査する。もし、すでに承認されていたならば、選挙管理者Aは二重投票として承認を拒否する。

【0015】

Step 2-3 選挙管理者Aは、署名検査器220を用いて、 s_i と e_i を検査する。もし、合格ならば、選挙管理者Aは、 e_i を署名作成器230に通して、署名 d_i

$$d_i = \sigma_A(e_i)$$

を計算し、 d_i を投票者 V_i の装置100に送信する。これにより投票者 V_i の承認を行う。また投票者リストに投票者 V_i を追加する（投票者リストは投票開始時に予めすべて空白とされてある）。

【0016】

Step 2-4 選挙管理者Aは、投票者リストと投票者数を公表する。

Step 3 投票者 V_i は、投票者装置100により投票用紙とその署名情報を以下のように作成する。

Step 3-1 投票者 V_i は、 d_i と r_i を乱数成分除去器150に入力して、投票用紙 x_i の署名情報 y_i

$$y_i = \delta(d_i, r_i)$$

を求める。

【0017】

Step 3-2 投票者 V_i は、署名検査器160を用いて、 y_i が選挙管理者Aの署名であることを確認する。もし、不合格であったなら、投票者 V_i は $\langle e_i, d_i \rangle$ を示すことにより、選挙管理者Aの不正を主張する。

Step 3-3 投票者 V_i は、前記署名確認が合格であれば $\langle x_i, y_i \rangle$ を集計者Cの装置300に匿名通信路500を用いて送信する。

Step 4 集計者Cは、集計者装置300により以下のようにして票を収集する。

【0018】

Step 4-1 集計者Cは、署名検査器310を用いて y_i が投票用紙 x_i の署名であることを確認する。もし、合格ならば、集計者Cは投票リスト60

0に、投票用紙 x_i とその署名 y_i を $\langle q, x_i, y_i \rangle$ と番号付けをして掲載する。

Step 4-2 すべての投票後、集計者Cはリスト600を公表する（このリストはすべての投票者からアクセスが可能であるとする）。

Step 5 投票者 V_i は、投票者装置100により以下のようにして検証を行う。

【0019】

Step 5-1 投票者 V_i は、リスト600に掲載された投票の数がStep 2-4で公表された投票者の数と一致するかを表検査器170で検査する。もし、不合格ならば、番号 q と乱数 r_i を公表して、選挙管理者Aの不正を主張する。

Step 5-2 投票者 V_i は、自らの投票用紙 x_i が、リスト600に掲載されているかを表検査器170で検査する。もし、掲載されていないならば、 $\langle x_i, y_i \rangle$ を公表することにより、集計者Cの不正を主張する。

Step 6 集計者Cは、集計者装置300により以下のようにして開票、および、集計を行う。

【0020】

Step 6-1 投票者 V_i からの投票用紙 x_i 、署名 y_i の受信開始後、前記不正の通知が所定時間内になれば、集計者Cは、投票用紙 x_i を復号化器330にて開票し、投票内容 v_i

$$v_i = \rho_C(x_i)$$

を求め、投票内容 v_i が正しい投票か、つまり投票内容 v_i が正しいフォーマットになっているかを検査する。

【0021】

Step 6-2 集計者Cは、投票内容 v_i を集計器340を用いて集計し、その結果を周知するとともに、図1cに示すように、 v_i をリストに追加する。

Step 7 投票者 V_i は、投票者装置100により集計者Cの操作が正しいことを確認する。つまり図1cに示すリスト中にすべての v_i が追加されたか、また投票者 V_i の x_i と v_i とが対応しているかを確認する。

【0022】

以下では、この発明の第二の実施例について説明する。

これの全体構成は第一の実施例における集計者装置300を分散集計者装置700としたものと同じである。通信シーケンス例や投票者装置100の構成例、選挙管理者装置300の構成例などは集計者装置300を分散集計者装置700とする以外は先と同様である。以下、図6に分散集計者装置700の構成例を示す。

【0023】

ここで、分散集計者の暗号関数 (ξ_C, ρ_C) は、それぞれの分散集計者が持つ鍵で復号化を行なうことで、暗号化された投票文が復号可能となったり、復号化に必要な人数にしきい値が存在し、一定数のしきい値付分散集計者が集まれば復号可能なようなものとする。

このような暗号関数については、例えばElGamal 暗号 (Taher ElGamal : "A public key cryptosystem and a signature scheme based on discrete logarithms", IEEE Transactions on Information Theory, Vol.IT-31, No.4, pp.469-472(July, 1985)) の暗号化関数と復号化関数があり、これの分散した復号者による復号の手法やしきい値を導入した手法についての詳細は、Yvo Desmedt, Yael Frankel : "Threshold cryptosystems" in Advances in Cryptology-CRYPTO '89, Lecture Notes in Computer Science 435, Springer-Verlag, Berlin, pp. 307-315(1990) に記述されている。

【0024】

以下、この発明の第二の実施例における投票の手順を示す。これは、第一の実施例のStep 6, 7を以下のように変更したものであり、Kは分散集計者の人数である。

Step 6 分散集計者 C_1, \dots, C_K は、分散集計者装置700により、以下のようにして集計を行う。

【0025】

Step 6-1 分散集計者 C_1, \dots, C_K は、投票用紙 x_i を分散復号化器730にて開票し、投票内容 v_i を例えば次のようにして求める。

$$x_{i1} = \rho_{C1}(x_i), x_{i2} = \rho_{C2}(x_{i1}), x_{i3} = \rho_{C3}(x_{i2}), \dots \\ \dots, v_i = \rho_{CK}(x_{iK-1})$$

求めた投票内容 v_i が正しい投票かを検査する。

【0026】

Step 6-2 分散集計者 C_1, \dots, C_K は、投票内容 v_i を集計器 740 を用いて集計し、その結果を周知するとともに、 v_i をリストに追加する。

Step 7 投票者 V_i は、投票者装置 100 により分散集計者 C_j の操作が正しいことを確認する。

以下では、この発明の第三の実施例について説明する。

【0027】

これの全体構成は第一の実施例における集計者装置 300 をしきい値付分散集計者装置 800 としたものと同一である。通信シーケンス例や投票者装置 100 の構成例、選挙管理者装置 300 の構成例などは集計者装置 300 をしきい値付分散集計者装置 800 とする以外は先と同様である。以下、図 7 にしきい値付分散集計者装置 700 の構成例を示す。

【0028】

以下、この発明の第三の実施例における投票の手順を示す。これは、第一の実施例の Step 6, 7 を以下のように変更したものであり、 K は分散集計者の人数、 L はしきい値である。

Step 6 しきい値付分散集計者 C_1, \dots, C_K は、しきい値付分散集計者装置 800 により、以下のようにして集計を行う。

【0029】

Step 6-1 しきい値付分散集計者 C_1, \dots, C_K は、投票用紙 x_i をしきい値付分散復号化器 830 にて開票し、投票内容 v_i を例えば次のように求める。分散集計者 C_1, \dots, C_K から任意に選んだ L 人の集計者を C_1, \dots, C_L とし、しきい値付分散復号化器 830 により、

$$x_{i1} = \rho_{C1}(x_i), x_{i2} = \rho_{C2}(x_{i1}), x_{i3} = \rho_{C3}(x_{i2}), \dots \\ \dots, v_i = \rho_{CL}(x_{iL-1})$$

を求め、投票 v_i が正しい投票かを検査する。ここで、しきい値付分散

復号化器 830 は L 個以上が作動すれば復号が可能であり、 L 未満であれば復号できないものとする。

【0030】

Step 6-2 しきい値付分散集計者 C_1, \dots, C_K は、投票内容 v_i を集計器 740 を用いて集計し、その結果を周知するとともに、 v_i をリストに追加する。

Step 7 投票者 V_i は、投票者装置 100 によりしきい値付分散集計者 C_j の操作が正しいことを確認する。

【0031】

ここで用いられた分散復号化器 730 としきい値付分散復号化器 830 は、例えば、上記の Desmedt-Frankel の方式を用いて構成されたものであり、例えば（しきい値）分散集計者 C_1, \dots, C_K でそれぞれ x_i を部分復号し、これらを 1 個所に集めて v_i を得るなど他の手法によってもよく、複数存在する（しきい値付）分散集計者間の通信等を必要とする場合がある。

【0032】

図 3 乃至図 7 に示す各装置はその機能構成を示したものであり、これら各機能を動作を順次行わせるための制御手段を備え、また全体乃至一部をコンピュータにより実行させることもできる。

【0033】

【発明の効果】

この発明では、投票内容（ v ）を集計者の暗号化鍵で暗号化しているので、投票者は投票内容を復号化させるために、鍵を送信する必要がない。

続いて、集計者を複数とした場合には、集計者全員の合意が得られなければ開票作業が開始されない。

【0034】

さらに、一定数の集計者が開票できる場合には、正当な集計者がある程度集まれば開票作業が開始でき、不正者もしくは故障者の影響を除去できる。

また、集計者が投票内容を改竄（かいざん）しても、公開された投票内容の一覧表を閲覧することで、投票内容の改竄を検出できる。すなわち、自らの投票が

利用されていないときには、暗号化された投票用紙 x_i と選挙管理者の署名 y_i を公開し、不正を主張すればよい。この際、不正な集計者の数が一定であるならば異議申し立て時のプライバシーは保証されている。

【0035】

さらに、複数の集計者をおいた場合に、この発明では、暗号化鍵を用いて、投票内容を暗号化して送信しているので、投票用紙の収集の際に、集計者が途中経過を漏洩して選挙に影響を及ぼすといった不正が防止できる。

以上より、この発明では集計者の暗号化鍵を用いて、投票者の利便性を向上させ、また、集計者を複数とすることにより、途中経過を漏洩して選挙に影響を及ぼすといった不正を解決できる。

【図面の簡単な説明】

【図1】

aはこの発明の全体構成を示すブロック図、b、cはそれぞれ投票内容一覧表の例を示す図である。

【図2】

この発明方法の処理手順における通信シーケンスを示す図。

【図3】

投票者装置100の機能構成例を示すブロック図。

【図4】

選挙管理者装置300の機能構成例を示すブロック図。

【図5】

集計者装置400の機能構成例を示すブロック図。

【図6】

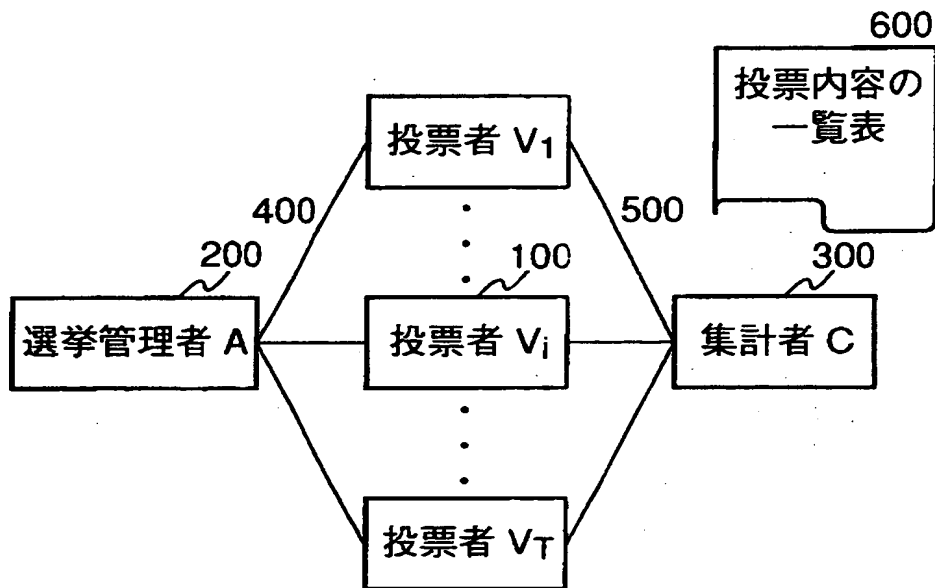
分散集計者装置700の機能構成例を示すブロック図。

【図7】

しきい値付分散集計者装置800の機能構成例を示すブロック図。

【書類名】 図面

【図 1】



a

番号	投票内容 (付加情報)
1	x_j, y_j
⋮	⋮
q	x_i, y_i
⋮	⋮

b

番号	投票内容 (付加情報)
1	x_j, y_j, v_j
⋮	⋮
q	x_i, y_i, v_i
⋮	⋮

c

図 1

【図 2】

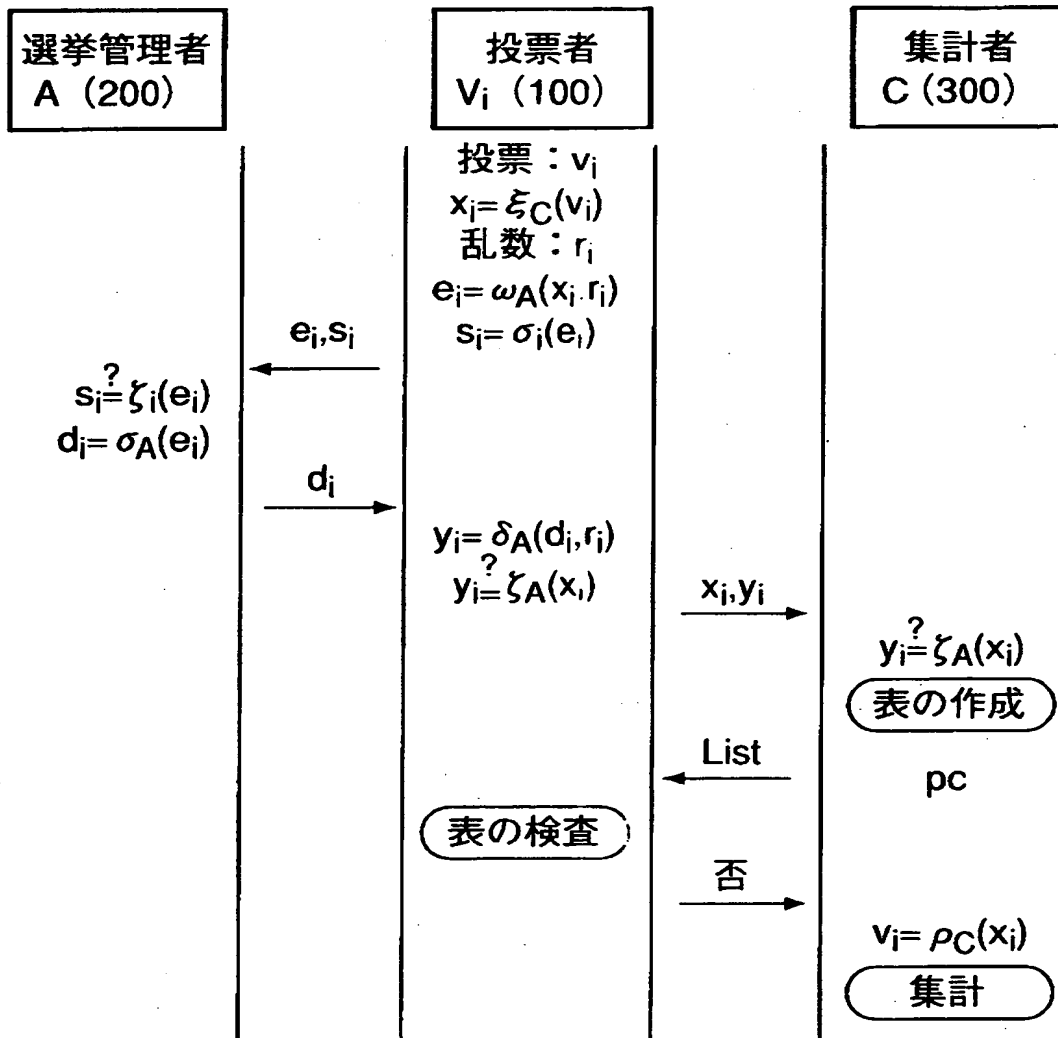


図 2

【図 3】

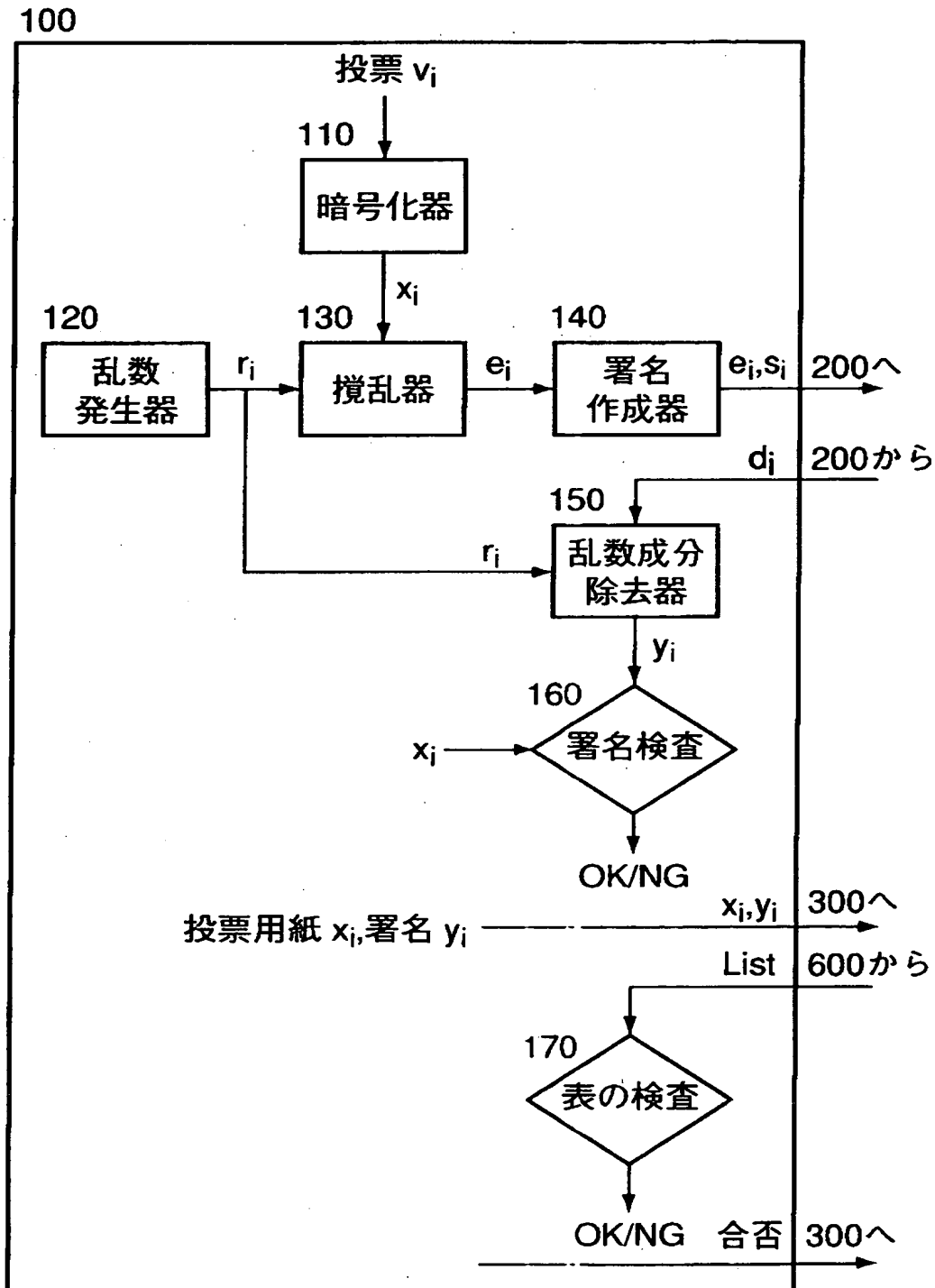


図 3

【図4】

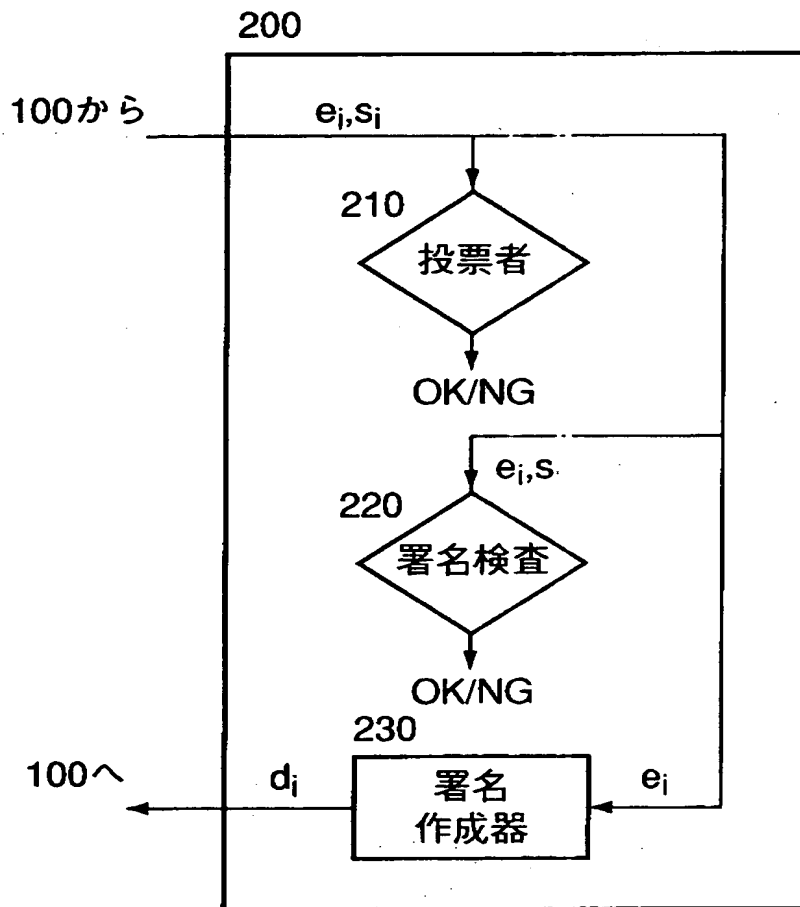


図 4

【図 5】

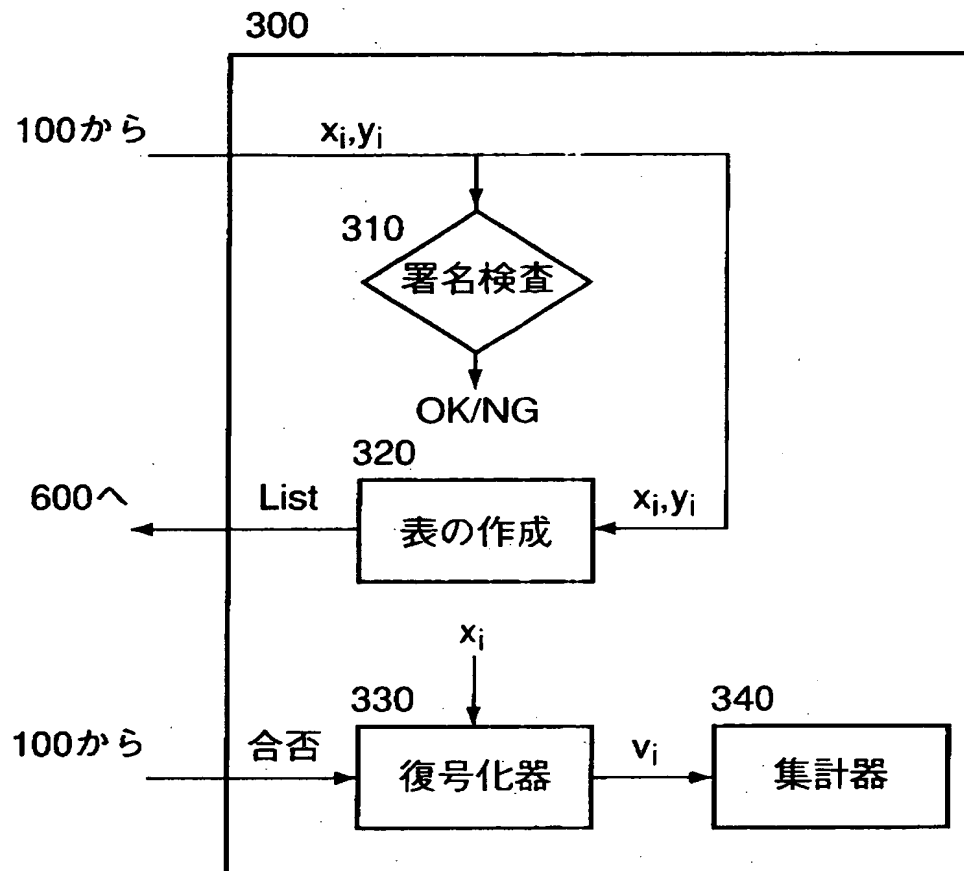


図 5

【図 6】

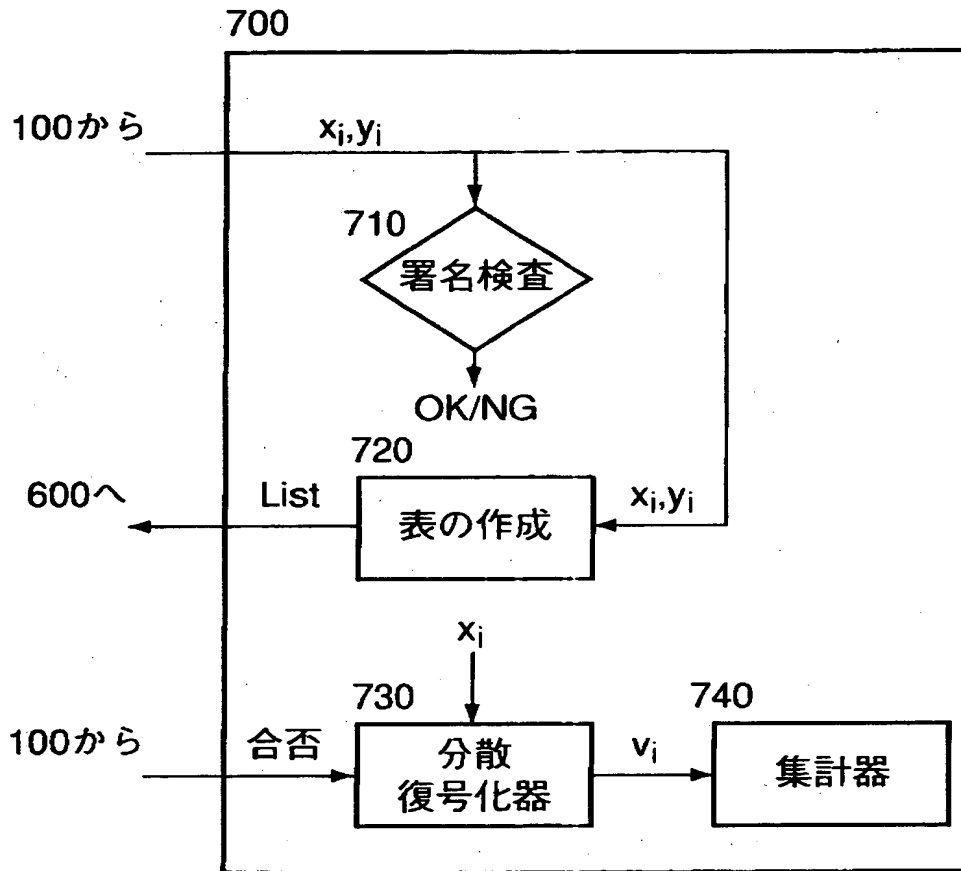


図 6

【図 7】

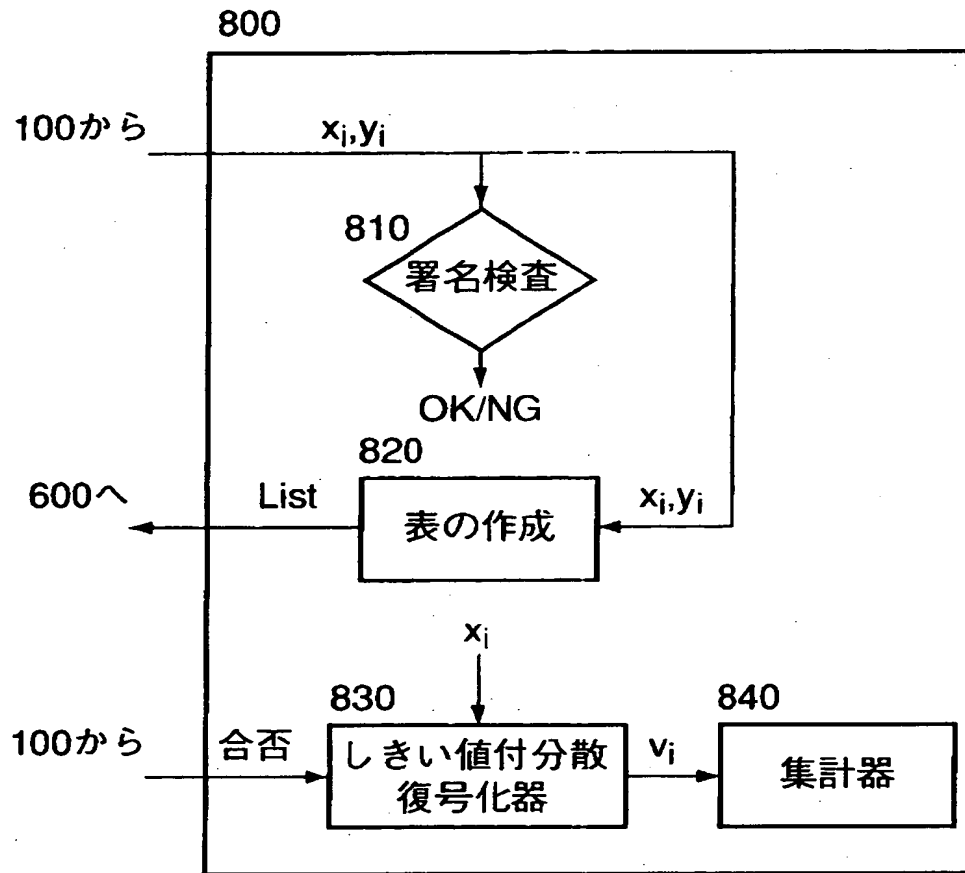


図 7

【書類名】 要約書

【要約】

【課題】 投票者 V_i は投票内容 v_i を復号化させるために鍵を集計者 C へ送る必要がない。

【解決手段】 V_i は v_i を C の鍵で暗号化し、その暗号化投票内容 x_i を乱数 r_i と共に攪乱して投票文 e_i を作り、その署名 s_i と e_i を選挙管理者 A へ送り、 A は e_i の署名 d_i を作成して V_i へ返し、 d_i から r_i の影響を除去した署名 y_i を得、 x_i 、 y_i を C へ送り、 C で y_i を検証し、合格したら x_i 、 y_i の表を作り、公開し、 V_i はその表を検査し、 x_i があることを確認し、 C は x_i を復号化して v_i を得、これを表に追加する。

【選択図】 図2

【書類名】 職権訂正データ
【訂正書類】 特許願

<認定情報・付加情報>

【特許出願人】

【識別番号】 000004226

【住所又は居所】 東京都新宿区西新宿三丁目19番2号

【氏名又は名称】 日本電信電話株式会社

【代理人】 申請人

【識別番号】 100066153

【住所又は居所】 東京都新宿区新宿四丁目2番21号 相模ビル

【氏名又は名称】 草野 卓

【選任した代理人】

【識別番号】 100100642

【住所又は居所】 東京都新宿区新宿4丁目2番21号 相模ビル 草
野特許事務所

【氏名又は名称】 稲垣 稔

出 願 人 履 歴 情 報

識別番号 [000004226]

1. 変更年月日 1995年 9月21日
[変更理由] 住所変更
住 所 東京都新宿区西新宿三丁目19番2号
氏 名 日本電信電話株式会社
2. 変更年月日 1999年 7月15日
[変更理由] 住所変更
住 所 東京都千代田区大手町二丁目3番1号
氏 名 日本電信電話株式会社